For Council: 13 June 2022 APPENDIX 1A

Lichfield City Council

Minutes of the Meeting of the Audit Committee held via 'Zoom'
on Thursday 9 June 2022 at 4.00pm

Present: Councillor C Spruce (Deputy Chair, in the Chair) and Councillors J Greaves, I Jackson, A Lax and M Warfield (Cllr M Warfield entered the meeting at agenda item 6/Minute 5).

In attendance: A Briggs (Town Clerk and RFO), G Keatley (Internal Auditor) and A James (Accounts Officer).

Apologies: Councillor A Smith.

1. DECLARATIONS OF INTEREST AND REQUESTS FOR DISPENSATION

None

2. MINUTES AND MATTERS ARISING

RESOLVED: The Minutes of the meeting held on 14 March 2022 be agreed as a correct record.

3. CYBER SECURITY POLICY

Members considered the revised Cyber Security Policy which included revisions discussed at the previous Audit Committee meeting. The Town Clerk confirmed that Two Factor Authentication (2FA) had been introduced for all LCC employees with an email account, and that the same process was being rolled out to Members, with 13 of 28 Members having completed the 2FA process at the time of the meeting.

The Deputy Chair asked how the responsibilities of end users as detailed in the policy would be conveyed to other parties, notably contractors. The Town Clerk confirmed that no access to LCC computer equipment would be given to any contractor other than MT Services who had assisted with the drafting of this policy.

RECOMMENDATION TO COUNCIL: That the revised Cyber Security Policy** [**APPENDIX 1** to these Minutes] **be adopted.

4. OUT-TURN REPORT AND STATEMENT OF ACCOUNTS

Members considered the Out-turn Report and the Draft Statement of Accounts (Annual Return), for the year ending 31 March 2022. The Town Clerk advised the Committee of potential changes to the draft Annual Return resulting from discussions with Mazars in regard to 'Objective L' (free to access website) on page 3 of the AGAR document; the statement on the AGAR seeming to contradict with the accompanying guidance and causing confusion as to whether the correct response is 'yes' or 'not applicable'. A definitive response from Mazars was awaited at the time of the meeting.

The Town Clerk also confirmed the need to amend the draft AGAR to confirm the City Council has met its responsibilities as a Trustee; the draft supplied not correctly reflecting this. The Town Clerk to make these amendments and include the final AGAR as an Enclosure to these minutes.

The Town Clerk then gave a brief overview of service performance against budget, noting in particular the overspend on Open Spaces as previously reported to Council, the relatively low staff costs of the Markets resulting from the use of agency staff to undertake basic duties only, and the relatively high rental income from the Markets as a result of the earlier than anticipated lifting of COVID restrictions.

The Committee noted the 'Total Service Costs' figure of £815,879 which excludes Repairs and Renewals and CIL, is very close to the 2021/22 precept figure of £816,400.

The Deputy Chair remarked that preparation of the 2021/22 budget was very difficult given the unknowns of COVID at the time. The Deputy Chair then asked that as normality returns and accurate budgets can be set, the focus on financial controls to meet those budgets be concentrated upon; the Town Clerk agreed that this was a priority following the uncertainty of the past two years.

Cllr A Lax enquired as to the recovery of Guildhall bookings; the Town Clerk confirmed a steady recovery was in progress but that income from 2021/22 reflected the Guildhall being open to some users throughout the financial year 2021/22, notably Slimming World and Mencap who are two of the hall's most regular users. Cllr A Lax stated that while some weddings will take place this year it is likely that some of those who delayed during COVID will have bookings for 2023 and that this should reflect well in Guildhall bookings for that year.

The Deputy Chair thanked all involved in preparing the year end accounts and supporting documentation.

RECOMMENDATION TO COUNCIL:

1 The Report and Out-Turn Statement 2021/22 be received.

2 The Council as Trustee of the Johnson Birthplace Charitable Trust make a payment of £12,936 from the Trust Funds to the City Council as the contribution to the expenditure incurred by the City Council in operating the Museum during the 2021/22 financial year.

3 In respect of the finalised External Auditor Annual Return for the year ending 31 March 2022 *[Enclosure 1 to these Minutes]:*

- ***a. The council approve the Annual Governance Statement (Section 1 of the Annual Return) and that this be signed by the Mayor and Town Clerk on behalf of the Council.***
- ***b. The Council approve the Accounting Statements (Section 2 of the Annual Return) and this be signed by the Mayor on behalf of the Council***
- ***c. The Council note the Annual Internal Audit Report section of the Annual Return***
- ***d. The Council note the dates for the exercise of public rights - commencing on 15 June 2022 and ending on 26 July 2022.***

The Chair entered the meeting at this point and gave apologies for late arrival.

5. LCC STANDING ORDERS AND FINANCIAL REGULATIONS

The Committee considered an updated Standing Orders and Financial Regulations document that incorporated:

- The removal of gender specific references
- Updates to legislative references
- CPI replacing RPI as the preferred method for calculating annual increases within the Financial Regulations document
- Other non-material amendments to ensure accuracy of the document

The Town Clerk advised of minor errors within the Standing Orders & Financial Regulations document as circulated (notably there being two Standing Order number 26). The Committee agreed that the Town Clerk make non-material amendments to rectify such errors prior to presentation to Council, and that the final version be circulated with these minutes.

The Deputy Chair asked that any amendments to documents in future be highlighted in order that the changes are more immediately obvious.

RECOMMENDATION TO COUNCIL: ***That the revised Financial Regulations and Standing Orders Document*** *[Enclosure 2 to these Minutes]* ***be adopted.***

6. DATE AND TIME OF NEXT MEETING

In the calendar of meetings as Thursday 8 December 2022 at 4.00pm via 'Zoom'.

THERE BEING NO FURTHER BUSINESS THE MEETING WAS CLOSED AT 4:18PM

Lichfield City Council

Cyber Security Policy

This policy is separated into three sections, the first being the technical measures in place to guard against attack, the second being the expectations of users to ensure they do not undermine the technical measures through negligent actions, and the third being a basic plan in the event of a successful attack.

Lichfield City Council operates a multi-layered approach to cyber security in order to reduce potential risks that are common to modern internet connected IT environments. In an online world it is necessary to take measures to protect against a multitude of different threats which vary in their methodology. This includes attacks that attempt to exploit flaws within software or hardware to socially engineered attacks that attempt to get users to unknowingly compromise their systems or partake in financial transactions with a non-genuine entity.

It is also recognised that despite having a broad defence, threats could still have an impact from a new vulnerability in software or hardware to which a resolution or even detection does not yet exist or from accidentally following a malicious link. As such it is also necessary to be prepared to respond to and recover from incidents that may happen.

1. Technical Detail

The purpose of this section of the document is to give a basic outline of the measures in place. Data is stored both online in cloud environments with major providers of online services and within the local network.

IT support is provided by MT Services Computer Systems Ltd who maintain the IT services mentioned herein.

Cloud environment

One use of a cloud environment is e-mail, which is both for transport and storage. The service provider has scanning implemented which reduces the risk of malicious content reaching an end user and serves to reduce the amount of spam e-mail.

In the event of a breach in the cloud environment actions can be taken to inhibit further propagation and the actions of the breach assessed and responded to appropriately.

There is a ransomware detection service implemented as an additional service in the remote monitoring software deployed by the IT support company.

Another service held within the cloud is the online backup service. As this relates to the data held on the local network this is expanded upon in the relevant section below.

Gateway

At the gateway level between the internet and the local network there is a firewall solution in place which has security services that inspects the traffic between the local network and the internet. The security services cover a broad spectrum of threat detection and response topics such as virus/malware, spyware, ransomware, intrusion prevention, botnet detection, content filtering, sandboxing and so on.

Local Network
At the local network level there is a software solution installed on the client machines and the server that covers viruses, malware, ransomware, spyware and other potentially unwanted applications on a file and data stream (internet or network access) level.
Client machines are subject to security policies set from the server regarding user passwords and access to locations containing sensitive or private data.

Both client machines and the server are subject to patch management for security updates (amongst other forms of updates) implemented by a remote monitoring platform deployed by the IT support company. As mentioned above there is an additional service running as part of this platform for ransomware detection.

In the event of a breach that affects the central data store on the server (such as encrypting ransomware) or if there is accidental deletion or a failure of the server there are both on-site and off-site backup solutions from which data or even the full server content can be recovered. In both on-site and off-site (cloud based) scenarios access to the backed-up data is restricted by both username and password and encryption keys to access the content.

Data Access
Any member of staff with access to an LCC logon can view the data held on the central system. However, sensitive information – mostly relating to staff – is password protected within its own drive and is only accessible by the Town Clerk and Deputy Town Clerk. MT Services confirm that as the Council's IT Administrators they can log on to see the data if they wish, but their own internal policies apply to such access. In the event of restricting access to MT Services it would be far more difficult for them to investigate and resolve any issues arising.

Support
In the event of suspicious activity or abnormal behaviour of the IT systems Lichfield City Council will inform the IT support company who will investigate and take corrective actions as necessary on the maintained systems. This is in addition to anything that may be detected by the automated systems in place.

2. Responsibilities of the End User
Despite strong protection via the IT support provider, there remains a considerable responsibility on the end user to be mindful of the potential threats and implications of security breaches and unauthorised access to information the City Council holds; like people, technology is not infallible, but with a combination of technical protection and employee responsibility, the chances for security breaches can be minimised.

The protection of confidential data and device security are significant considerations, the loss of such data potentially leading to a multitude of potential consequences both for those whose data has been compromised and for the Council as a whole. There are a number expectations that City Council employees, Councillors, contractors or anyone else with any level of access to LCC IT equipment are expected to comply with:

LCC owned equipment:
- All Council owned devices to be password protected (minimum of 8 characters)
- All devices to be secured prior to leaving them unattended

- No City Council owned electronic devices (including flash drives) to be removed from Council premises without the express authorisation fo the Town Clerk or Deputy Town Clerk
- No confidential information to be sent to any third party without the express consent of the Town Clerk or Deputy town Clerk
- Passwords should not be shared with colleagues unless there is an urgent business need; in the event of such need, the password to eb changed at the first available opportunity thereafter. Any request to share a password must be from either the Town Clerk or Deputy Town Clerk
- If an email or other electronic communication contains banking details for payment, the details to be verified prior to any payment being made

Personal Equipment

- Employees may be required to use personal devices to access company systems (e.g. sharing photographs taken on a site visit by phone to the central system). Such occurrences must be kept to a minimum, and if it is envisaged that such a requirement would be relatively frequent, the employee to discuss the appropriateness of the provision of LCC equipment for this purpose with the Town Clerk.
- No personal device to be connected to the City Council network without the express consent of the Town Clerk or Deputy Town Clerk.

Email Security

The City Council operates individual email accounts for the majority of its employees and all serving LCC Councillors. All City Council email addresses are to be protected by Two Factor Authentication (2FA) as a minimum. This applies equally to email accounts utilised by officers and members.

Any individual with access to such an account (whether personal or communal) is required to:

- Verify the legitimacy of each email, including in particular the email address and sender name
- Avoid opening any links, attachments or emails that appear suspicious
- Avoid clickbait titles and links
- Contact the Town Clerk regarding any suspicious emails at the first opportunity

NB: any remote access to LCC systems (for example to aid home working) must also be protected by 2FA as a minimum.

3. Attack Management Plan

In the event of a suspected or confirmed cyber-attack, the Town Clerk must be contacted at once.

Instructions are provided in the Server Room at Donegal House to allow staff to disconnect the Sonicwall and therefore isolate LCC systems in the event of an attack.

The Town Clerk will be the responsible officer, charged with liaising with the City Council's IT providers to assess the significance of the breach and the appropriate next steps in the given circumstance. If the Town Clerk is unavailable, some or all of these matters would become the responsibility of the Deputy Town Clerk. As a minimum, the Town Clerk must:

- Notify other senior members of staff of the potential/confirmed breach (to include Deputy Town Clerk, Civic Officer and Accounts Officer)

- Inform the Leader and Deputy Leader of the Council and keep them apprised of developments (all members of Council to be advised at the first opportunity wherever possible)
- Ensure all potentially affected third parties are notified as soon as practicable
- Report the matter to the Information Commissioners Office and the Police as appropriate
- Implement the recommendations of the IT provider wherever practicable in response to the threat
- Ensure that normal service is resumed as soon as practicable, via the backup facilities mentioned in section 1 of this document. If such backup is unavailable, a central 'hub' to be established in conjunction with the IT provider to allow the basic business of the Council to continue, including the continuation of follow up procedures relating to the breach.
- Provide a written report to Council detailing the origin of the breach and measures implemented/to be implemented to minimise the likelihood of a similar scenario occurring in the future.

City Council officers will be guided by the expert advice of the IT support provider. In general this policy supports a presumption in favour of following the advice given by the IT support provider in relation to new or updated software/hardware that can enhance the security of the City Council's systems. The Town Clerk will assess the cost/benefit in the first instance, with recourse to Council as necessary.

It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore all employees and Councillors MUST take personal responsibility and make considered judgements in how they utilise LCC equipment. If in any doubt they should seek clarification from the Town Clerk, Deputy Town Clerk or the City Council's IT support provider.